Data Analytic Core
Privacy Policies

Accountability, Audit and Risk Management

1 DAC Governance and Privacy Program

The Data Analytic Core:

a. Appoints the Director of the DAC as the Senior Official for Privacy. This individual is accountable for developing, implementing, and maintaining data governance and privacy in compliance with federal privacy laws and policy. The Director monitors federal privacy laws and policy for changes that affect the DAC privacy program.
b. Allocates funding in support of these activities to:
    1. Data Analytic Core Director for leadership and oversight of planning, monitoring, and decision-making;
    2. Data Analytic Core Compliance Coordinator for administrative operational implementation; and
    3. Data Analytic Core Infrastructure Programmer/Analyst for technical implementation.
c. Develops a strategic plan for implementing privacy controls,
d. Develops, disseminates, and implements its privacy policies and procedures; and
e. Updates the privacy plan annually or as needed in between.

2 Risk Management Framework and Impact Assessment

2.1 Framework

The DAC:

a. Categorizes its information system according to the data classification level designated by Dartmouth College. According to this classification, the DAC Information Resources (data) are considered Level 3: *strictly confidential, requiring the highest level of sensitivity. This includes FERPA data, personally identifiable information (PII), personal health information (PHI), credit card information (PCI), among others.*

b. Selects and implements security and privacy controls at the moderate level according to NIST SP800-53.

c. Assesses the privacy and security controls, including privacy continuous monitoring; and

d. Obtains approval by the Dartmouth College Vice Provost for Institutional Research and the Chief Information Security Officer prior to operation for any new or changed system that will collect, process, share, and/or store PII/PHI.

3 Privacy Impact Assessment

The DAC:

a. Ensures a Privacy Impact Assessment ascertains risk to individuals resulting from collection, sharing, storing transmitting, use, and disposal of PHI/PII;
b. Conducts a Privacy Impact Assessment for its Information System, programs, Information Resources, and any other activities that pose a potential risk for disclosure;
c. Reviews the Privacy Impact Assessment annually.

4 Requirements for Contractors and Service Providers

The DAC does not allow any third-parties access into its Information System.

5 Privacy Monitoring and Auditing

The DAC:

a. Monitors and audits privacy controls annually to ensure its effectiveness and that it is up-to-date with current federal and state laws, as well as international laws where applicable.
b. Documents, tracks, and ensures mitigation of corrective actions are implemented through annual monitoring or auditing.

The DAC maintains all elements of PHI and PII in its secure Information System with access limited to authorized Users only and on a need-to-know basis for the purposes of approved research by both the Data Owner and CPHS.

6 Privacy Awareness and Training

The DAC:

a. Develops, implements, and updates a comprehensive privacy training and awareness program with the goal of ensuring that all Users understand privacy responsibilities and procedures.
b. Conducts the training annually and is targeted based on role.
c. Upon completion of the annual training, all Users must pass an exam and sign an acknowledgement and acceptance of responsibility for ensuring the protection of PHI/PII every year.

7 Privacy Reporting

The DAC reports all significant changes to its privacy program that contains:

a. A description of the purpose for which the DAC is establishing or modifying the privacy program and an explanation of how the scope of the program is commensurate with the purpose;
b. The authority under which the program will be maintained;
c. An evaluation of the impact of the proposal on PHI/PII;
d. Explanation of how each new change is compliant with the Privacy Act; and
e. A description of how the collected information will be maintained.

8 Privacy-Enhanced System Design and Development

a. The Dartmouth Information Security Group ensures the Dartmouth College Information, Technology, and Consulting team implements the DAC Information System to support privacy controls throughout the life cycle of a project using DAC Information Resources. The technical systems (networks, physical environment, and other technical infrastructure) are designed to incorporate privacy concerns with any significant changes to the system.

b. In collaboration with the DAC Director, the Dartmouth Information Security Group ensures the Dartmouth College Information, Technology, and Consulting team conducts periodic reviews of the systems to determine any updates to maintain compliance with the Privacy Act.

9 Accounting of Disclosures

The only time the DAC would disclose PHI/PII would be as required by federal law in an investigation or if there were an incident. In the case of an incident, all disclosures would be tracked in the incident tracker and breach notification made to the Data Owner in compliance with the Data Use Agreement and Federal Law.

The DAC:

a. Maintains an accurate accounting of disclosures of information held in its Information System, including:
    1. Date, nature, purpose of each disclosure
    2. Name and address of the person or agency to which the disclosure was made.
b. Retains the accounting of disclosures for the life of the record or 5 years after the disclosure; whichever is longer; and
c. Makes the accounting of disclosures available to the person names in the record upon request.